Claims

What is claimed is:

1. A method for transmitting data, the method comprising:

encrypting a payload;

adding a header to the payload to form a data packet;

encrypting the payload and the header of the data packet so that the payload is at least twice-encrypted and the header is at least once-encrypted;

transmitting the data packet only after at least twice encrypting the payload.

2. The method of claim 1, wherein the encrypting a payload further comprises encrypting the payload with a symmetric key.

3. The method of claim 1, further comprising:

receiving the data packet at a first device;

performing a first decryption of the data packet at the first device;

forwarding the data packet to a second device;

performing a second decryption of the payload at the second device.

4. The method of claim 1, further comprising:

creating a symmetric session key;

wherein the payload is encrypted with the symmetric session key.

5. The method of claim 1, wherein the transmitting further comprises transmitting the data packet over a wireless link.

6. A device for transmitting data, comprising:

a wireless transceiver;

an encryption engine coupled to the wireless transceiver for encrypting a payload according to a first encryption algorithm, adding a header to the payload to form a data packet, and encrypting the data packet according to a second algorithm;

a processor coupled to the encryption engine and to the wireless transceiver and configured to execute the encryption algorithms.

7. The device of claim 6, further comprising a receiver coupled to the processor for receiving the data to be transmitted.

8. The device of claim 6, wherein the payload further comprises location information regarding the location of the wireless device.

9. The device of claim 6, wherein the first encryption algorithm employs a symmetric key.

10. A method comprising:

generating a symmetric session key at a first device;

encrypting the symmetric session key at the first device using a public key associated with a second device;

transmitting the encrypted session key to the second device;

decrypting the encrypted session key at the second device using a private key associated with the public key;

encrypting a payload using the symmetric session key at the first device;

adding a header to the payload to form a data packet at the first device;

encrypting the payload and the header of the data packet to form an encrypted data packet at the first device;

transmitting the encrypted data packet from the first device.

11. The method of claim 10, further comprising:

receiving the encrypted data packet at a third device;

decrypting data packet at the third device to form a decrypted data packet, the decrypted data packet having an encrypted payload;

forwarding the decrypted data packet to the second device;

decrypting the payload at the second device using the decrypted session key.

12. The method of claim 10, wherein transmitting further comprises transmitting the data packet over a wireless link.

13. The method of claim 10, wherein the first device comprises a wireless device and the second device comprises a wireline device.

14. The method of claim 10, wherein the second device comprises a server.

15. The method of claim 10, wherein the payload includes location information.

16. The method of claim 10, wherein the generating a symmetric session key at a first device further comprises generating the symmetric session key based on a random number.

17. The method of claim 10, wherein the encrypting a payload using the symmetric session key employs at least one of the encryption algorithms DESX or DES.

18. A method for transmitting data, the method comprising:

encrypting a payload using a first key;

adding a header to the payload to form a data packet;

encrypting the payload and the header of the data packet with a second key;

transmitting the data packet.

19. The method of claim 18, wherein the first key further comprises a symmetric key.

20. The method of claim 18, wherein the encrypting a payload further comprises encrypting the payload using at least one of the encryption algorithms DESX or DES.

21. A method comprising:

generating a symmetric session key at a first device;

encrypting the symmetric session key at the first device using a public key associated with a second device;

transmitting the encrypted session key to the second device;

decrypting the encrypted session key at the second device using a private key associated with the public key;

encrypting at least a portion of a data packet using the symmetric session key at the first device to form an encrypted data packet;

transmitting the encrypted data packet from the first device.

22. The method of claim 21, wherein the transmitting the encrypted data packet further comprises transmitting the encrypted data packet over a wireless link.

23. The method of claim 21, wherein the first device comprises a wireless device and the second device comprises a wireline device.

24. The method of claim 21, wherein the second device comprises a server.

25. The method of claim 21, wherein the data packet includes location information.

26. The method of claim 21, wherein the generating a symmetric session key at a first device further comprises generating the symmetric session key based on a random number.

27. A device comprising:

a processor;

a wireless transceiver coupled to the processor for transmitting an encrypted data packet to a server;

a memory coupled to the processor, the memory having a public key associated with the server permanently stored therein;

wherein the processor encrypts the encrypted data packet using the public key.

28. A device comprising:

means for encrypting a payload;

means for adding a header to the payload to form a data packet;

means for encrypting the payload and the header of the data packet so that the payload is at least twice-encrypted and the header is at lease once-encrypted;

means for transmitting the data packet only after at least twice encrypting the payload.

29. A computer readable medium, comprising program instructions for performing a method comprising:

encrypting a payload;

adding a header to the payload to form a data packet;

encrypting the payload and the header of the data packet so that the payload is at least twice-encrypted and the header is at least once-encrypted;

transmitting the data packet only after at least twice encrypting the payload.